Cambium Networks™

Integrating External Captive Portal with On-Premise cnMaestro API

Table of contents

Chapter 1 Contents

Introduction 3
Feature Details 3
Workflow 4
3rd party certificate loading on cnMaestro: 5
Configuration 7
For deployments where cnMaestro hostname entry cannot be added to the DNS Server forward zone. 9

Introduction

Guest access WLAN is designed specifically for BYOD (Bring your own device) setup, where large organizations have both staff and guests running on same WLAN or similar WLANs. Cambium Networks Provides different options to the customers to achieve this based on where the captive portal page is hosted and who will be validating and performing authentication process.

They are 3 locations where the captive portal page can be hosted:

1. Internal Access Point (Limited customization like Logo and Background Image)
2. External Hotspot (External 3rd party Web/Cloud hosted captive portal, fully customized)
3. cnMaestro (Semi customized portal, with additional features like SMS Authentication, Payment Gateways and Vouchers)

Authentication Methods:

1. Clickthrough (Portal page with a button to accept terms & conditions and get internet access)
2. RADIUS (External Authentication server like, Windows NPS / IAS or Free RADIUS)
3. LDAP (Authenticate using LDAP/Active Directory)
4. Local Guest Account (Single username /password stored on Access Point)

In this document, we will be specifically talking about External Hotspot integrating with on-premise cnMaestro to securely POST the user credentials to authenticate the user using External RADIUS

Since the secure POST needs installation of certificate and installing certificate in each AP's in a big deployment is not straightforward, we are providing the option to install certificate in a single point(cnMaestro) for the whole network. Another benefit is this option also opens up the flow where the external portal can directly POST to cnMaestro and have the login flow completely done between client and the external portal which gets ways the issues with cross origin requests which are getting slowly blocked on browsers.

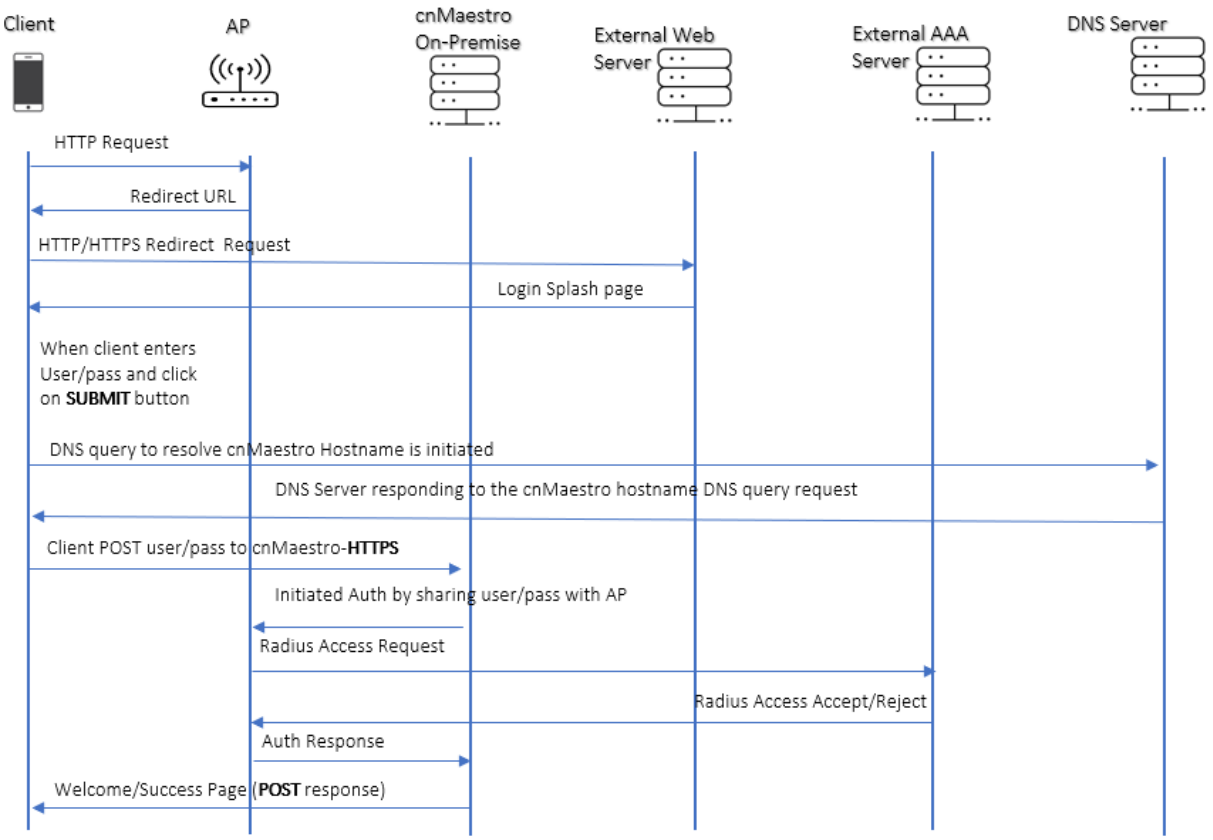
Feature Details

Customers who wanted a secure communication channel to authenticate the user securely should choose to POST the user credentials to cnMaestro. To enable this feature, one must enable External Portal Post Through cnMaestro available in Guest Access.

UI Screenshot:

Workflow

A general workflow when an external webserver and cnMaestro is configured to accept **HTTPS POST** messages from client.



This setup consists of below main parts:

1. Supplicant (Wireless clients- Laptops, mobile phones etc)
2. External Web Server
3. DNS server
4. On-Premise cnMaestro
5. Authenticator (Cambium Access Point)

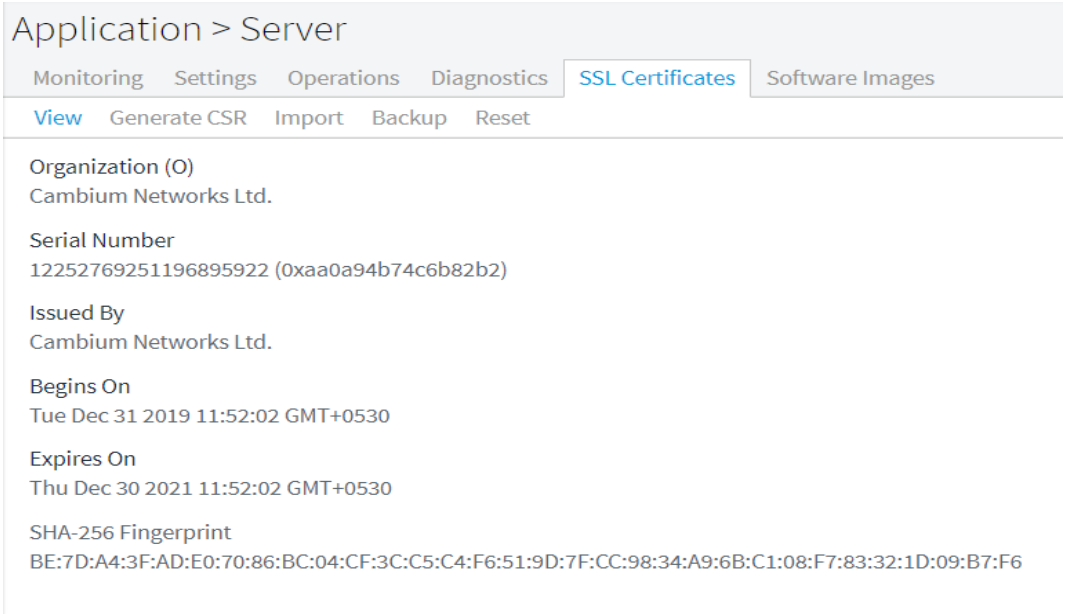
6. Authentication Server (RADIUS)

A certificate needs to be loaded on the cnMaestro for secure communication between clients and cnMaestro.

3rd party certificate loading on cnMaestro:

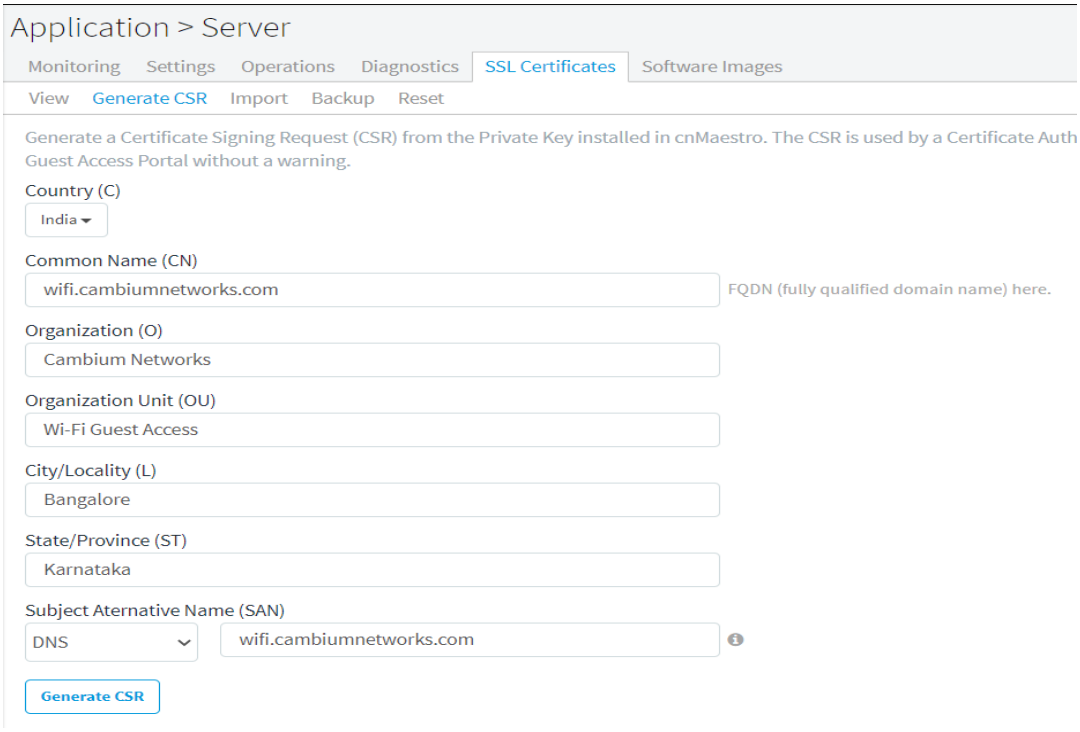
cnMaestro comes with a self-signed certificate. Customers would want this to change to a trusted certificate to provide the secure login page for their users.

Self-signed certificate already available in the cnMaestro.

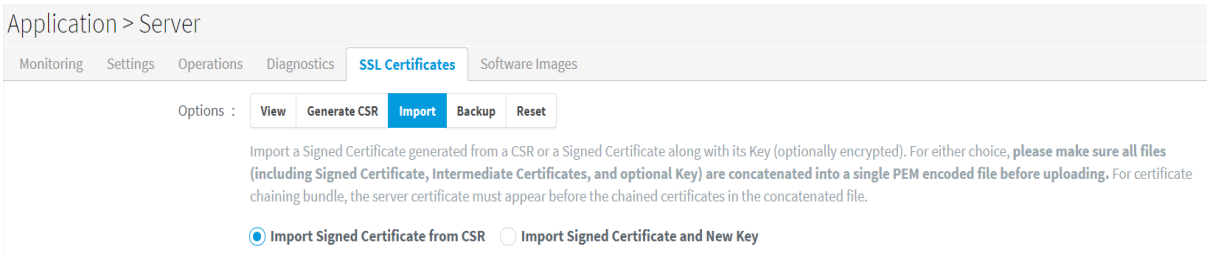


Steps to load a 3rd party certificate on cnMaestro is as follows

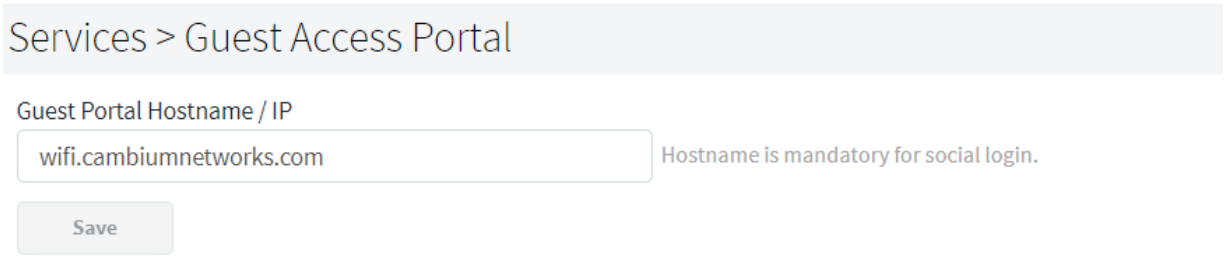
1. Generate a CSR.



2. Once the signed certificate is received from the 3rd party, load it onto the cnMaestro.



3. After loading the certificate, change the guest portal's URL to reflect the new hostname.

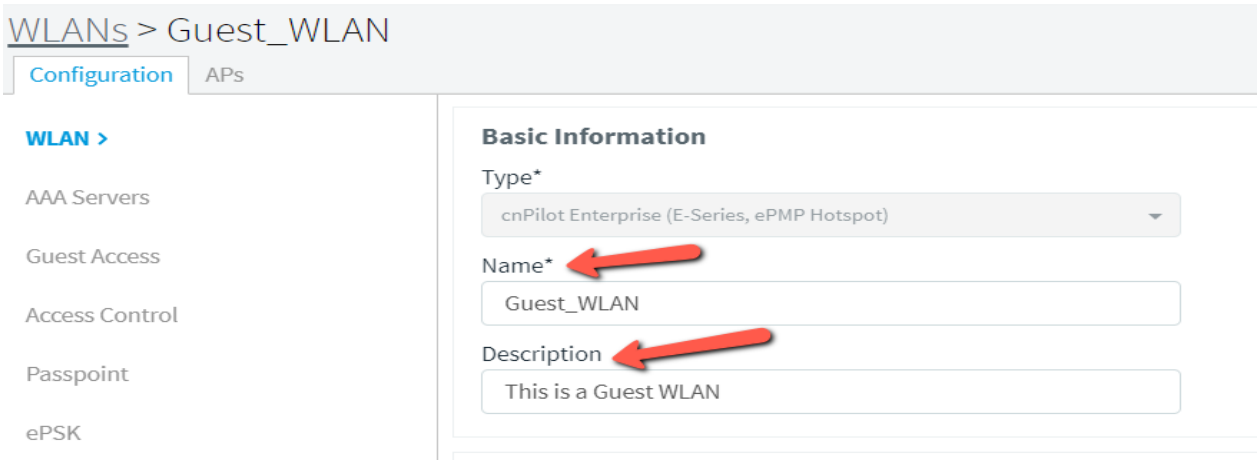


Note: DNS Server forward zone should be updated with an entry to point to the cnMaestro hostname. This will ensure that when client tries to contact the redirected URL (which AP provides to contact cnMaestro) external DNS can send a query response.

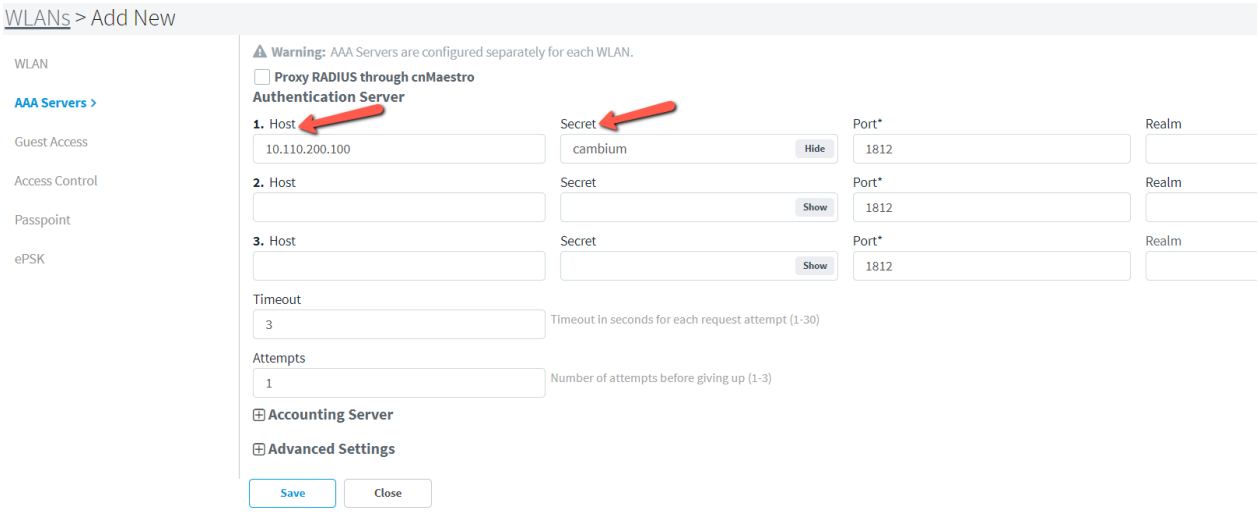
Configuration

1. On cnPilot Access Points: Configure >> WLAN
2. On cnMaestro: Shared Settings/ WLANs and AP Groups >> WLANs

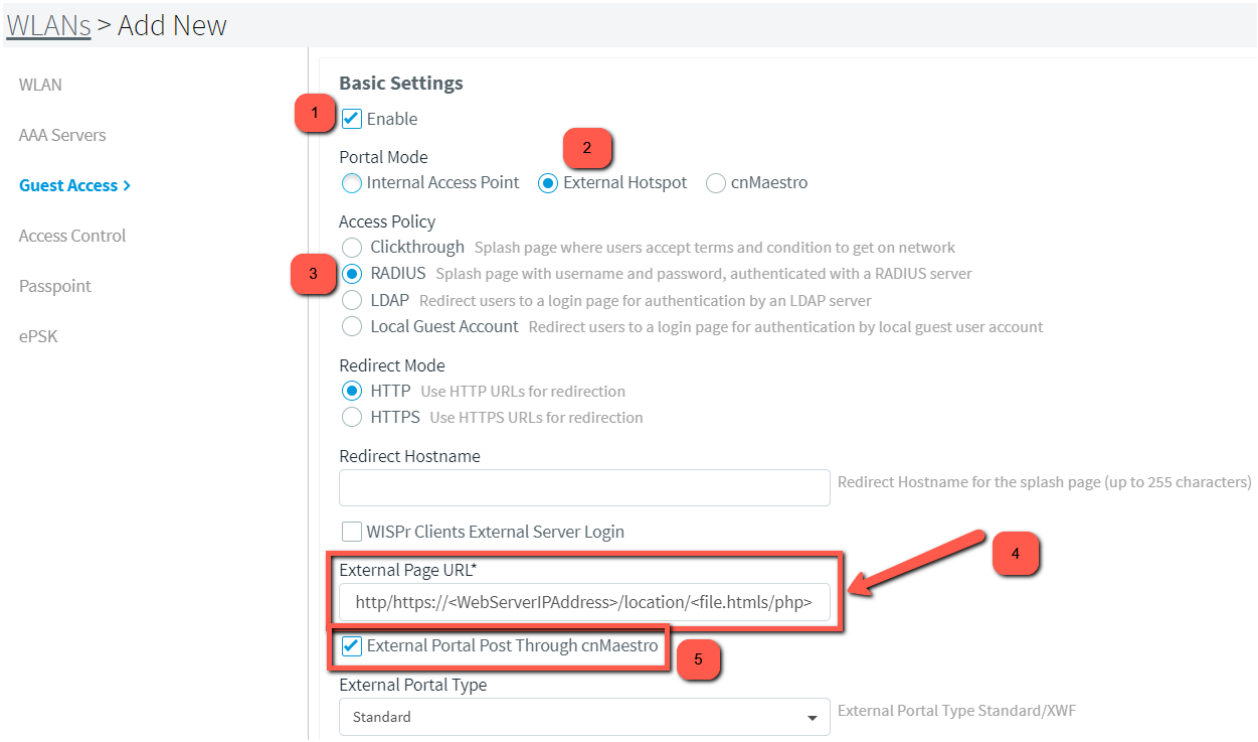
WLAN: Key in the **WLAN name** and **description**. By default, WLAN Name is taken as **SSID Name**.



AAA Server: Key in the AAA server setting like **IP address (RADIUS server)** and **shared secret** (This shared secret should match to the secret created on RADIUS server).



Guest Access: Enter the URL of captive portal hosted on external web server and select other required parameters.



Example External page URL

1. IP address: http://10.110.200.100:8000/login_cnMaestro.html
2. URL : https://dev.xyznetworkmanager.com/portal/index.php?hotspotname=laCambium

Portal Page hosted on Webserver should perform a POST **to cnMaestro** from the **client.**

NOTE: HTTPS POST to cnMaestro is supported only on the on-premise version.

Login request must be sent to below URL over standard HTTPS port 443:

"https://cnMaestroHostName/cn-ctlr/ext-guest/ga-ext-login?<query_string_append>"

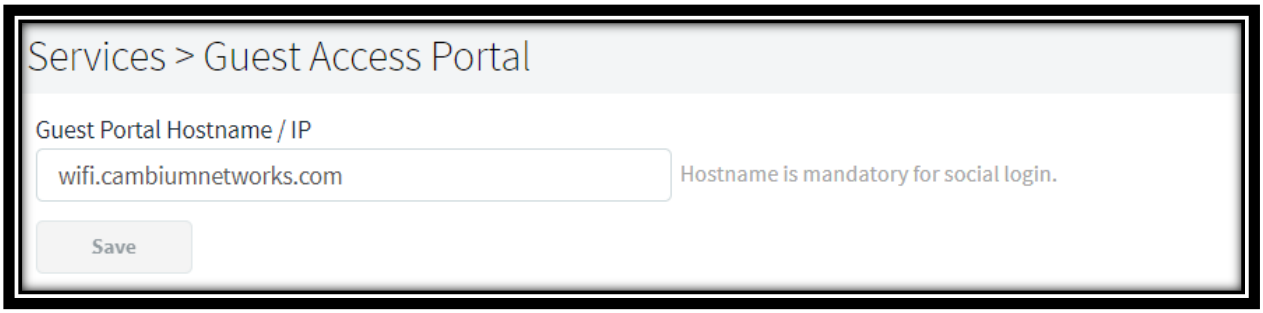
Logout request to be sent on below URL over standard HTTPS port 443:

"https://cnMaestroHostName/cn-ctlr/ext-guest/ga-ext-logout<query_string_append>"

Please replace the cnMaestroHostname with the value as found in ga_srvr query string in the redirection URL and add the same query string in this request.

The ga_srvr in the query strings points to the cnMaestro hostname/IP address what ever has been configured in the cnMaestro guest portal hostname config settings.

cnMaestro hostname can be found at cnMaestro Guest Portal settings



Here in this example configuration, the cnMaestro hostname is "wifi.cambiumnetworks.com"

Real time POST message for the above cnMaestro configuration is as follows

https://wifi.cambiumnetworks.com/cn-ctlr/ext-guest/ga-ext-login?ga_ssid=Guest_WLAN&ga_ap_mac=58-C1-7A-6E-DE-A1&ga_nas_id=E425-6EDEA1&ga_srvr=wifi.cambiumnetworks.com&ga_cmac=E4-A7-A0-D4-31-C2&s=0wOu3Y7xiarheIDTFytHsAGQsGRkzRU2b_b5vh3GmNCI.&ga_Qv=eUROBR86HBgAGDEEVgQAGw4UWRUCACYVMgFPRy5ZXlFfUSVGWS9FVghZRyRLBhMUMww.

Note that, everything received as part of query string (everything after question mark) in the redirection URL, needs to be appended back in the POST URL.

For deployments where cnMaestro hostname entry cannot be added to the DNS Server forward zone.

Note: IP reachability between the client and cnMaestro is must for client to POST the user credentials

- AP can be configured as a Proxy DNS to respond to the client's DNS query.
- Only CLI support is added for this proxy feature.
- This is available from 3.11.4.1-r3 and 4.1-x(yet to release) releases.

The commands should be added in Guest WLAN as below,

guest-access redirect user-page <cnMaestroIPaddress>

guest-access redirect user-page hostname <cnMaestroHostname>

Example configuration screenshot:

```
E410-0DA1AF(config)#
E410-0DA1AF(config)# wireless wlan 1
E410-0DA1AF(config-wlan-1)#
E410-0DA1AF(config-wlan-1)#
E410-0DA1AF(config-wlan-1)# guest-access redirect user-page 10.110.200.83
E410-0DA1AF(config-wlan-1)# guest-access redirect user-page hostname wifi.cambiumnetworks.com
E410-0DA1AF(config-wlan-1)# save
[Config Save OK]
E410-0DA1AF(config-wlan-1)#
```

Guest WLAN CLI configuration screenshot: